Task Order GSQ0016AJ0074
Modification PS12
September 1, 2017

Marine Corps Enterprise Network Cyber Defense Support Services

in support of

Marine Corps Cyberspace Operations Group

Issued to
Northrop Grumman

Against
GSA Alliant Government-wide Acquisition Contract
GS00Q09BGD0056
DUNS #015247885

Issued by
General Services Administration
Federal Systems Integration and Management Center (FEDSIM)
1800 F Street, NW
Suite 3100 (QF0B)
Washington, D.C. 20405

Awarded
June 03, 2016

C.1 BACKGROUND

The Marine Corps Cyberspace Operations Group (formerly Network Operations and Security Center (MCNOSC)) is an operational and staff organization supporting the global Marine Corps Enterprise Network (MCEN) Command and Control (C2) capabilities for Fleet Marine Forces and garrison forces stationed around the world, as well as joint forces within the Joint Information Environment (JIE). MCCOG is designated as the Marine Corps' Computer Network Defense (CND) Service Provider (CNDSP) and has been fully accredited by the Defense Information Systems Agency (DISA) since the inception of the CNDSP program. In this role, the MCCOG executes defensive cyber operations on the global MCEN and joint networks to include protection, detection, response and sustainment functions in alignment with the DOD Directive O-8530.01, DOD O-8530.01-M, and DOD Instruction O-8530.02 which serve as the CNDSP program's governing directives.

MCCOG's Operations Branch includes the Defensive Cyber Operations Section (DCOS) which is responsible for all technical CNDSP functions. DCOS assigned duties encompass the full range of CND functions from incident handling to malware analysis and sensor signature management. The DCOS operates 24 by 7 centralized command and control (C2) of CND personnel and assets to achieve speed of action and uniformity of controls. Additionally, the DCOS directly oversees the application of information assurance (IA) controls and enterprise CND services for all out-sourced information technology (IT) vendors supporting Marine Corps systems and enclaves per DOD Instruction 8500.01, dated March 14, 2014.

C.1.1 PURPOSE

The primary purpose of this Task Order (TO) is to support MCCOG in carrying out the technical subset of the doctrinal DoD CNDSP functions of protection, detection and response in order to disrupt, deny and degrade network adversaries' ability to influence the confidentiality, integrity, availability, authentication and non-repudiation of IT services provided to users on the MCEN and joint networks.

C.2 SCOPE

The scope of this TO supports the MCCOG DCOS by analyzing network traffic, identifying malicious and unauthorized activity, and responding to intrusion incidents; implementing, configuring, operating, and maintaining network defense systems; and auditing MCEN network security controls, managing enterprise vulnerabilities, drafting formal direction for review and ensuring compliance with enterprise remediation measures. The scope of this TO also includes operations of the DCOS internal workforce training program and maintaining a workforce consistent with DOD IA workforce standards, per the DOD Directive 8570.01-M. The primary location of work is Quantico, VA, with secondary sites in Camp Pendleton, CA and Kansas City, MO. Additional travel may be required per section F.4.

C.3 MCCOG OPERATIONAL ENVIRONMENT

C.3.1 MCCOG POLICIES AND GUIDANCE

The MCCOG Cyber Defense support program is guided by the latest DOD policies and procedures in IA and CND, which includes those referenced throughout the performance work statement (PWS):

- Marine Corps Order 5239.2B, "Marine Corps Cybersecurity", dated 19 May 2015 or later. (included in attachment V)
- Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01B, "Cyber Incident Handling Program," dated 10 Jul 2012 or later. (included in attachment V)

- DoD 8570.01-M, "Information Assurance Workforce Improvement Program" (dated 24 Jan 2012 or later) or succeeding DoD training directive. (included in attachment V)
- Secretary of the Navy Instruction (SECNAVINST) 5239.19, "Department of the Navy Computer Network Incident Response and Reporting Requirements", dated 18 Mar 2008 or later or later. (included in attachment V)
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-115, "Technical Guide to Information Security Testing and Assessment," dated 30 Sep 2008 or later. (included in attachment V)
- CJCSM 6510.03, "Department of Defense Cyber Red Team Certification and Accreditation," dated 28 Feb 2013 or later. (included in attachment V)
- Marine Corps Warfighting Publication 5-1, "Marine Corps Planning Process," dated 24 August 2010 or later. (included in attachment V)
- Joint Publication 3-12 (R), "Cyberspace Operations," dated 5 February 2013 or later.
- Marine Corps Order P3500.72A, "Marine Corps Ground Training and Readiness (T&R) Program," dated 18 April 2005 or later. (included in attachment V)
- Secretary of the Navy Manual (SECNAV-M) 5216.5, "Department of the Navy Correspondence Manual," dated June 2015. (included in attachment V)
- DoD Directive O-8530.01, Cybersecurity Activities Support to DoD Information Network Operations, March 7, 2016
- DoD O-8530.01-M, "Department of Defense Computer Network Defense Service Provide Certification and Accreditation Program", 17 December 2003

The MCCOG is the Marine Corps' designated Tier II CNDSP Service provider as directed in the SECNAVINST 5239.19 "Department of the Navy Computer Network Incident Response and Reporting Requirements", dated 18 Mar 2008 or later, and the Marine Corps Order 5239.2B "Marine Corps Cybersecurity", dated 19 May 2015.

The DoD 8570.01-M "Information Assurance Workforce Improvement Program" (dated 24 Jan 2012 or later) provides MCCOG the guidance on implementing and maintaining a qualified IA workforce. The CNDSP program established architecture (referenced in CJCSM 6510.01B, "Cyber Incident Handling Program," dated 10 Jul 2012) is the DoD manual and foundation for the MCCOG Cyber Defense program.

C.3.2 MCCOG CYBER DEFENSE TRAINING, TOOLS AND TECHNOLOGIES

The following attachments are provided in Section J to provide the Contractor details of the MCCOG Cyber Defense environment:

- Section J, Attachment S (Tools and Technology Inventory) – provides a list of general tools and technologies applicable to the performance of this task order.
- Section J, Attachment T (Sample Training Calendar) – provides a sample of the annual course list.

C.4 TASKS

C.4.1 TASK 1 – PROVIDE PROGRAM MANAGEMENT

The Contractor shall provide program management support under this TO. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this PWS. The Contractor shall identify a Program Manager (PM) by name who shall provide onsite management, direction, administration, quality control, and leadership of the execution of this TO. The Contractor shall perform all activities necessary to ensure the accomplishment of timely and effective support by

implementing productivity and management methods ("timely" and "effective" means the activities meet the minimum mandatory requirements identified in CJCSM 6510.01B, “Cyber Incident Handling Program,” dated 10 Jul 2012 or later, and SECNAVINST 5239.19 “Department of the Navy Computer Network Incident Response and Reporting Requirements”, dated 18 Mar 2008 or later.

C.4.1.1 SUBTASK 1 – COORDINATE A PROJECT KICK-OFF MEETING

The Contractor shall schedule and coordinate a Project Kick-Off Meeting (Section F, Deliverable 02) at the location approved by the Government. The meeting will provide an introduction between the Contractor personnel and Government personnel who will be involved with the TO. The meeting will provide the opportunity to discuss transition, technical, management, and security issues, and travel authorization and reporting procedures. At a minimum, the attendees shall include the Contractor’s Key Personnel, representatives from MCCOG and directorates, other relevant Government personnel, and the GSA Federal Systems Integration Management (FEDSIM) contracting officer’s representative (COR). The Contractor shall provide the following at the Kick-Off meeting:

a. Brief Status of Transition Activities
b. Quality Control Plan (QCP) – (Section F, Deliverable 08)

C.4.1.2 SUBTASK 2 – PREPARE A MONTHLY STATUS REPORT (MSR)

The Contractor shall develop and provide an MSR (Section F, Deliverable 06) using Microsoft (MS) Office Suite applications, by the tenth of each month via electronic mail to the Technical Point of Contact (TPOC) and the COR. The MSR shall include the following:

a. Activities during reporting period, by task (include: on-going activities, new activities, activities completed; progress to date on all above mentioned activities). Start each section with a brief description of the task.
b. Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them.
c. Personnel gains, losses, and status (security clearance, etc.).
d. Government actions required.
e. Schedule (show major tasks, milestones, and deliverables; planned and actual start and completion dates for each).
f. Summary of trips taken, conferences attended, etc. (attach Trip Reports to the MSR for the reporting period).
g. Incurred cost for each CLIN up to the previous month.
h. Projected cost of each CLIN for the current month.

C.4.1.3 SUBTASK 3 – CONVENE TECHNICAL STATUS MEETINGS

The Contractor PM shall convene a monthly Technical Status Meeting with the TPOC, COR, and other Government stakeholders. The purpose of this meeting is to ensure all stakeholders are informed of the monthly activities and MSR, provide opportunities to identify other activities and establish priorities, and coordinate resolution of identified problems or opportunities. The Contractor PM shall provide minutes of these meetings, including attendance, issues discussed, decisions made, and action items assigned, to the COR within five workdays following the meeting.

C.4.1.4 SUBTASK 4 – PREPARE A PROJECT MANAGEMENT PLAN (PMP)

The Contractor shall document all support requirements in a PMP.

The PMP shall:

a. Describe the proposed management approach
b. Contain detailed Standard Operating Procedures (SOPs) for all tasks
c. Include milestones, tasks, and subtasks required in this TO
d. Provide for an overall Work Breakdown Structure (WBS) and associated responsibilities and partnerships between or among Government organizations
e. Include the Contractor's Quality Control Plan (QCP)
f. Include the Contractor's Communication Management Plan (CMP)
g. Include the Contractor's Risk Management Plan (RMP)
h. Include the Contractor's Integrated Master Schedule (IMS)

The Contractor shall provide the Government with a draft PMP (Section F, Deliverable 04), on which the Government will make comments. The final PMP (Section F, Deliverable 05) shall incorporate the Government's comments.

C.4.1.5 SUBTASK 5 – UPDATE THE PROJECT MANAGEMENT PLAN (PMP)

The PMP is an evolutionary document that shall be updated annually at a minimum. The Contractor shall work from the latest Government-approved version of the PMP.

C.4.1.6 SUBTASK 6 –TRIP AFTER ACTION REPORTS

The Government will identify the need for a Trip Report (Section F, Deliverable 07) when the request for travel is submitted. The Contractor shall keep a summary of all long-distance travel including, but not limited to, the name of the employee, location of travel, duration of trip, and point of contact (POC) at travel location. All trips made by the Contractor on behalf of the program require an After Action Report (AAR) (Section F, Deliverable 28) to be submitted 7 business days from the date of return. The format and summary of information to provide in this AAR is provided in Section J, Attachment Y.

C.4.1.7 SUBTASK 7 – UPDATE QUALITY CONTROL PLAN (QCP)

The Contractor shall update the QCP submitted with their proposal and provide a final QCP as required in Section F, Deliverable 08. The Contractor shall periodically update the QCP, as required in Section F, as changes in program processes are identified.

C.4.1.8 SUBTASK 8 – STAFFING PLAN

The Contractor shall verify all personnel certifications status on a monthly basis (Section F, Deliverable 11). The Contractor shall provide a staffing plan with the names of all individuals supporting the TO by task area and functional support role, and include a copy of the latest Training Management Plan.

C.4.1.9 SUBTASK 9 – TRANSITION-IN

All transition activities will be completed 30 calendar days after the start date of the order. The Contractor shall ensure that there will be minimum service disruption to vital Government business and no service degradation during the 30 day transition period. The Contractor shall deliver an updated Transition-In Plan (Section F, Deliverable 03) within five workdays of task order start.

C.4.1.10 SUBTASK 10 – TRANSITION-OUT

The Transition-Out Plan shall facilitate the accomplishment of a seamless transition from the incumbent to an incoming contractor/Government personnel at the expiration of the TO. The Contractor shall provide a Transition-Out Plan NLT 90 calendar days prior to expiration of the

TO (Section F, Deliverable 25). The Contractor shall identify how it will coordinate with the incoming contractor and/or Government personnel to transfer knowledge regarding the following:

a. Project management processes
b. Points of contact
c. Location of technical and project management documentation
d. Status of ongoing technical initiatives
e. Appropriate contractor–to-contractor coordination to ensure a seamless transition.
f. Schedules and milestones
g. Actions required of the Government.

The Contractor shall also establish and maintain effective communication with the incoming contractor/Government personnel for the period of the transition via weekly status meetings.

C.4.1.11 SUBTASK 11 – CONTRACTOR MANPOWER REPORTING

The Contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for the USMC via a secure data collection site. The Contractor is required to completely fill in all required data fields using the following web address: http://www.ecmra.mil/.

Reporting inputs will be for the labor executed during the period of performance during each Government fiscal year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year, beginning with 2013. Contractors may direct questions to the help desk at help desk at: http://www.ecmra.mil/.

C.4.2 TASK 2 – DISCOVERY AND COUNTER-INFILTRATION (D&CI)

The Contractor shall provide support in Incident Management, Hunt, and Cyber Threat Analysis Cell (CTAC) to defend the Marine Corps Enterprise Network (MCEN). This tasking will support the detection and response to all malicious activity throughout the MCEN to include classified environments.

C.4.2.1 SUBTASK 1 – INCIDENT MANAGEMENT (IM)

C.4.2.1.1 CYBER WATCH AND INCIDENT RESPONSE SUPPORT

The Contractor shall provide 24 x 7 x 365 support to conduct real-time analysis of ongoing IA / CND events on the MCEN, identifying incidents and making recommendations to protect the MCEN. The Contractor shall lead efforts in collecting and analyzing network and computing events presented via numerous sources in order to identify and document malicious or unauthorized activity on the MCEN. The Contractor shall conduct initial, formal incident reporting (outlined in CJCSM 6510.01B, “Cyber Incident Handling Program,” dated 10 Jul 2012 or later) and documenting technical details in the Marine Collections Database (MCD). The Contractor shall appropriately resolve daily incidents tracked in the MCD. The Contractor shall use appropriate skills and techniques in scoping, containing and eradicating incidents based on the processes outlined in CJCSM 6510.01B, “Cyber Incident Handling Program,” dated 10 July 2012 or later. Additionally, The Contractor shall be responsible for supporting the transition of network defense configurations as informed by resolved incidents in order to prevent future occurrences. The Contractor shall be responsible for continuity of services as data sources, analysis tools, and techniques will evolve to changes in the Marine Corps’ technical computing

environment as well as by mandates from US Cyber Command (USCYBERCOM). These efforts will support the analysis and correlation of over 414 million events per day (on average). During calendar year 2014, this resulted in over 4,295 incidents detected and handled within the MCEN. On average, each incident lasted 14.08 days. The Contractor shall perform 24x7x365 support from the primary site in Quantico, VA. Additional on-site support is required at the secondary location in Camp Pendleton, CA (see F.5 for shift schedule).

The Contractor shall:

a. Maintain the body of documentation that describes DCOS Computer Network Defense (CND) Watch Support and Incident Response tactics, techniques and procedures (Section F, Deliverable 16).
b. Receive and analyze network alerts and reports from multiple sources and determine possible causes of such alerts.
c. Monitor external data sources to maintain visibility of net defense threat conditions and emerging threats to the MCEN.
d. Inspect, identify and analyze network traffic for possible malicious and anomalous network activity.
e. Coordinate with MCCOG DCOS staff and outsourced IT-based process vendor personnel to investigate and validate network alerts.
f. Analyze log files from a variety of sources within the MCEN to characterize anomalous activity.
g. Conduct initial troubleshooting of network sensor availability and coordinate with DCOS Sensor Grid Support technicians to maintain sensor availability.
h. Recommend refinements to user-defined signatures for network sensors to enhance overall effectiveness of the MCEN sensor grid.
i. Recommend refinements to event correlation rules for implementation on the MCEN security information and event manager (SIEM).
j. Document the technical details utilizing internal reporting database of suspected network incidents to support incident response and reporting requirements (Section F, Deliverable 12).
k. Perform event correlation using information gathered from multiple sources within the MCEN to gain situational awareness and determine the impact of a network attack.
l. Notify DCOS Managers and appropriate parties of critical network incidents articulating the event's history, status, and potential impact.
m. Support post-mortem analysis of the magnetic and optical media collected from compromised systems.
n. Collect and analyze network intrusion artifacts from a variety of sources to include logs, system images and packet captures to enable mitigation of network incidents within the MCEN.
o. Perform initial forensic sound collection of system images to develop mitigation and remediation actions on the MCEN.
p. Coordinate with and provide expert technical support to USMC Information Assurance managers, on-site technicians and outsourced IT-based process vendor technicians to restore integrity to the MCEN.
q. Coordinate with intelligence analysts to correlate threat assessment data.
r. Document and report incidents within the MCD from initial detection through final resolution using standard DoD incident reporting methods (refer to CJCSM 6510.01B, "Cyber Incident Handling Program," dated 10 Jul 2012 or later).

s. Perform incident triage to determine scope, urgency, and potential operational impact by identifying the specific vulnerability and making recommendations which enable rapid remediation at the enterprise level.
t. Serve as technical experts and liaisons to external incident response personnel and brief incident details as necessary.
u. Provide remote incident handling support such as forensics collections, intrusion correlation tracking, threat analysis and direct system remediation tasks to on-site personnel.
v. Develop and publish incident response guidance and high-quality incident reports to appropriate audiences.
w. Upon resolution of network incidents, create custom signatures or correlation rules to detect future incidents as well as make MCEN protection recommendations to enhance passive resistance to future attack.
x. Maintain the deployable CND toolkit and stand prepared to support the DCOS fly-away team to conduct onsite support (approximately once every six months) to respond to critical CND incidents in accordance with SECNAVINST 5239.19 "Department of the Navy Computer Network Incident Response and Reporting Requirements", dated 18 Mar 2008 or later.
y. Provide support required to maintain the MCCOG's CNDSP accreditation per the standards set forth in the CNDSP program manual, DOD O-8530.1-M, (dated 17 Dec 03 or later) to include documentation and technical writing support as needed.

C.4.2.1.2 ADVANCED INCIDENT HANDLING

The Contractor shall provide 24 x 7 x 365 support and is responsible for the technical execution of incident handling functions as well as directly responding to severe network incidents. The Contractor shall deploy various techniques to discover and resolve evidence of malicious activity and open vulnerabilities on the MCEN. Technical execution shall align with CJCSM 6510.01B, "Cyber Incident Handling Program," dated 10 Jul 2012 or later. The Contractor shall be responsible for continuity of services as data sources, analysis tools, and techniques evolve to changes in the Marine Corps' technical computing environment as well as by mandates from USCYBERCOM.

The Contractor shall:

a. Maintain the body of documentation that describes DCOS CND Senior Analyst tactics, techniques and procedures (Section F, Deliverable 16).
b. Support the implementation of the latest CND policies, regulations, and compliance documents specifically related to network protections policies of the USMC, Department of the Navy (DON) and DoD.
c. Prepare detailed recommendations for network defense improvements to close or mitigate incidents on the MCEN.
d. Review and validate incidents tracked on the MCD.
e. Provide incident reports, summaries, and other situational awareness information as required.
f. Directly manage severe network incidents (e.g., coordinate documentation, work efforts, resource utilization within the organization) from inception to final after action reporting.
g. Conduct event trend analysis to identify breaches of the MCEN and coordinate with DCOS Incident Response to resolve compromises of the network.
h. Review incident reporting and intelligence products from adjacent and higher DoD CNDSP organizations to develop new methods of identifying attacks against the MCEN.

i. Make recommendations to the DCOS Sensor Grid Support Section to enhance network defense configurations on a daily basis.
j. Coordinate with certification and accreditation authorities, network managers, and system administrators and IA managers to correct policy infractions.
k. Make recommendations concerning the overall improvement of network security posture through changes in IT service provisioning on a weekly basis (Section F, Deliverable 37).
l. Interface with external organizations (e.g., public affairs, law enforcement, Command or Component Inspector General) to ensure appropriate and accurate dissemination of incident and other CND information.
m. Recommend enterprise protection measures based on incident trends.
n. Maintain a deployable CND toolkit and stand prepared to lead the DCOS fly-away team in conducting onsite support (approximately once every six months) during critical incidents as required per SECNAVINST 5239.19 "Department of the Navy Computer Network Incident Response and Reporting Requirements," dated 18 Mar 2008 or later.
o. Provide support required to maintain the MCCOG's CNDSP accreditation per the standards set forth in the CNDSP program manual, DoD O-8530.1-M, (dated 17 Dec 03 or later) to include documentation and technical writing support as needed.

C.4.2.2 SUBTASK 2 –HUNT TEAM

The DCOS Hunt Team is responsible for defensive cyber counter-infiltration operations against Advanced Persistent Threats (APT) within the MCEN. The Contractor shall be responsible for operations and sustainment functions to DCOS Hunt Team operations to include Server/Host, Network, and Planning. On average, 10 operations are executed per year at a length of 4-6 weeks each.

The Contractor shall:

a. Maintain the body of documentation that describes the tactics, techniques and procedures that comprise the Hunt team (Section F, Deliverable 16).
b. Assess and identify Advanced Persistent Threat (APT) activities within an Operating System (OS).
c. Develop and document tactics, techniques, and procedures (TTPs) for resource planning, operations, and analysis.
d. Research, identify, and verify new APT TTPs to strengthen the overall security posture of the MCEN.
e. Conduct Hunt planning utilizing the Marine Corps Planning Process, per the standards set forth in the Marine Corps Planning Process, MCWP 5-1 (dated 24 August 2010) to include documentation and planning support as needed.
f. Directly manage Hunt operations (e.g., coordinate documentation, work efforts, resource utilization within the organization) from inception to final after action reporting by leading the technical efforts of the Hunt Team.

C.4.2.3 SUBTASK 3 - CYBER THREAT ANALYSIS CELL (CTAC)

The Contractor is responsible for providing support to the CTAC, which serves as the principle supporting entity to all tailored incident response operations. This analytical cell, which consists of the malware and forensic analysis and exploit analysis teams, executes all advanced analysis for Marine Corps defensive operations.

C.4.2.3.1 MALWARE AND FORENSICS SUPPORT

The Contractor is responsible for responding to incidents using appropriate techniques in Surface Analysis, Runtime Analysis, and Static Analysis. The Contractor shall adhere to the procedures

outlined in CJCSM 6510.01B, "Cyber Incident Handling Program," dated 10 Jul 2012 or later for disk/drive image dissection processes. Additionally, the Contractor shall support the transition of network defense configurations as informed by resolved incidents in order to prevent future occurrences. The Contractor is responsible for maintaining currency as data sources, analysis tools, and techniques evolve to changes in the Marine Corps' technical computing environment as well as by mandates from USCYBERCOM. During calendar year 2014, the MCCOG team completed over 132 forensic investigations and analyzed over 371 malicious files.

The Contractor shall:

a. Maintain the body of documentation that describes DCOS CND Incident Response tactics, techniques and procedures, to include an emphasis on Malware and Forensic Analysis (Section F, Deliverable 16).
b. Support post-mortem analysis of the magnetic and optical media collected from compromised systems.
c. Perform initial, forensically sound collection of system images and inspect same to discern possible mitigation and remediation of network incidents on the MCEN.
d. Perform remote incident handling support such as forensics collections, intrusion correlation tracking, threat analysis and direct system remediation tasks to on-site responders.
e. Develop and publish malware and forensic analysis guidance and high-quality incident reports to appropriate audiences.
f. Provide sound forensic analysis on all devices during malware identification and provide feedback in relation to findings.
g. Provide surface and runtime analysis on newly acquired malware to develop new indicators in support of security posture changes to the MCEN.
h. Provide malware analysis to develop incident timelines to include: the dates and times of significant events, command and control domains, and call back addresses; threat objective; and compromised hosts and data.
i. Support custom signature and correlation rules creation to enhance MCEN protections.
j. Support the creation of a 'big data' analysis program through the identification of attributes and indications of targeted activity for profile development within the deployed DCOS sensor grid.
k. Analyze Malware to determine its capabilities, intent, indicators and origin.
l. Reverse engineer the sequence of events of a breach or attack.
m. Reverse engineer malware, using Dynamic and Static analysis.
n. Create alerts and identify indicators of compromise to facilitate detection and prevention of similar attacks.
o. Research new attacks and exploits.
p. Identify trends in incidents and malware to DCOS leadership.
q. Safeguard evidence, remediate and report incidents in accordance with approved USMC and DoD procedures.
r. Document findings; provide reports which incorporate intelligence information provided by the MCCOG Intelligence branch, historical attack information, as well as current and future (projected/possible) threats targeting the MCEN.
s. Provide support required to maintain the MCCOG's CNDSP accreditation per the standards set forth in the CNDSP program manual, DoD O-8530.1-M, (dated 17 Dec 03 or later) to include documentation and technical writing support as needed.

C.4.2.3.2 EXPLOIT ANALYSIS

The Contractor shall be responsible for providing capabilities necessary to review exploit code, their associated vulnerabilities, discover enterprise security discrepancies, assessing associated risk and assisting in the development of remedial action in coordination with the Mitigation Action Team. This team will conduct a thorough analysis of the capabilities and effects of adversary tactics, techniques, and procedures within the MCEN in order to improve the overall defense posture. This team will also support the discovery of vulnerabilities in the production environment including no-notice external security assessments.

The Contractor shall:

a. Create and maintain the body of documentation that describes the tactics, techniques and procedures that comprise the MCEN Exploit Analyst team (Section F, Deliverable 16).
b. Personnel supporting this task shall obtain a certification in MCCOG Red Team Level 1 course (See Table 1 Training Requirements) to further develop expertise on network attack methods.
c. Prioritize mitigation actions based on assessed risk upon discovery of critical exploits and vulnerabilities within the lab and production environments.
d. Conduct, analyze and review penetration tests and MCCOG/Joint Red Team assessment results to develop recommendations to protect the MCEN.
e. Analyze and review application, system, and network security postures across the MCEN in both lab and production environments through active scanning, application-layer protocol fingerprinting or traffic analysis.
f. Evaluate identified targeted environments in the MCEN for compliance with applicable DoD, DON, and USMC IT Security Policies (i.e. Secure Technical Implementation Guides)
g. Support the development and implementation of enterprise mitigation actions in response to complex vulnerabilities.
h. Develop the processes and procedures for and maintain a lab environment with current MCEN network and defensive configurations in order to test adversary tactics, techniques, and procedures against a mock MCEN (space, software, hardware and relevant configurations provided by government).
i. Develop the processes and procedures for replaying network attacks/compromises within a lab environment in order to scope the situation and develop recommended mitigation actions.
j. Support the creation of a repeatable data analysis process which identifies attributes and indications of targeted activity for profile development within the DCOS sensor grid.
k. Provide support required to maintain the MCCOG's CNDSP accreditation per the standards set forth in the CNDSP program manual, DoD O-8530.1-M, (dated 17 Dec 03 or later) to include documentation and technical writing support as needed.

C.4.3 TASK 3 –SENSOR GRID SUPPORT (SGS)

The Contractor shall be responsible for providing support to the Sensor Grid Support (SGS) team. Activities in support of this task include Host Security, Sensor Management, Signature Management and supporting development roles. The Contractor shall be responsible for the installation, operation, and maintenance of all defensive cyber infrastructure on the MCEN. The MCEN currently includes approximately 9,500 SIPRNet hosts and approximately 115,000 NIPRNet Hosts. There are 85 sites connected to the NIPRNet portion of the MCEN and 35 sites with SIPRNet connectivity. There are total of 200 network sensors within the MCEN sensor grid. Additionally, 22 Web Application Firewalls (WAF) are implemented in key locations across the enterprise network.

C.4.3.1 SUBTASK 1 –HOST BASED SECURITY (OPTIONAL TASK)

The Contractor shall leverage the host protection software directed for use by the USCYBERCOM to review events and logs to detect anomalies. The Contractor shall scan systems for vulnerabilities and indications of compromise. The Contractor shall be responsible for providing reports to the appropriate compliance mandated by USCYBERCOM. The Contractor shall be responsible for overall compliance, identification of anomalies and coordination with Signature Management personnel to develop custom host-based signatures to automate the detection of events of interest.

The Contractor shall:

a. Maintain and refine the body of documentation that describes DCOS Host Based Security section tactics, techniques and procedures (Section F, Deliverable 16).
b. Monitor host-based detection consoles for events of interest on end systems and provide anomaly reports to the DCOS Incident Management.
c. Assess endpoints on the enterprise network to meet DoD malware scanning and HBSS compliance requirements.
d. In coordination with the MCCOG CND Plans office, participate in the planning and implementation of new host based technology on the enterprise network.
e. Provide daily reports to DCOS leadership detailing trends in host compliance, anomaly activity and vulnerability statistics.
f. Maintain a test environment with all host assessment applications and innovate techniques to detect events of interest across the MCEN.
g. Maintain and ensure DCOS ePolicy Orchestrator servers are configured, analyzed, monitored and adequately patched in accordance with applicable DoD directives.
h. Install, operate, maintain, and troubleshoot HBS agents, modules, extensions, deployment tasks, and tags in order to provide required functionality to defend the MCEN.
i. Support the Host Assessment Team (HAT) on a weekly basis to analyze systems on the MCEN to identify vulnerabilities, anomalous host behavior, compromised network hardware and advanced malware.
j. Provide support required to maintain the MCCOG's CNDSP accreditation per the standards set forth in the CNDSP program manual, DoD O-8530.1-M, (dated 17 Dec 03 or later) to include documentation and technical writing support as needed.
k. Maintain compliance with the standards required by DISA Command Cyber Readiness Inspection (CCRI) in accordance with DISA and USCY guidelines.

C.4.3.2 SUBTASK 2 – NETWORK SENSOR SUPPORT

The Contractor shall ensure system availability, and conduct system administration, installation, troubleshooting and configuration support for MCEN network defense sensors and scanners, including all hardware and software used to conduct CNDSP functions throughout the MCEN. The Contractor shall provide 24 x 7 x 365 Network Sensor Support coverage from the primary site in Quantico, VA. Additional on-site support is required at the secondary location in Camp Pendleton, CA (see F.5 for shift schedule).

The Contractor shall:

a. Maintain and refine the body of documentation that describes DCOS Network Sensor Support Technicians' tactics, techniques and procedures (Section F, Deliverable 16).
b. Perform system administration of specialized network defense systems to include installation, configuration, maintenance, backup and restoration.
c. Identify potential conflicts with implementation and integration of specialized network defense systems within the network to protect the overall availability of the MCEN.

d. Maintain a network defense test environment to evaluate new applications, signatures, rules, filters and configurations of managed network defenses systems.
e. Create, maintain, and refine network traffic flow diagrams for the enterprise network which reflect the current state of all security applications.
f. Manage user accounts and permissions on MCEN network defense sensors and scanners.
g. Provide network defense system implementation, installation and configuration support to USMC installations and forces operating in deployed environments.
h. Provide detailed and near real time reporting on the status and availability of network sensors deployed across the MCEN.
j. Conduct life-cycle management on the body of enterprise defensive configurations.
k. Provide SIEM subject matter expertise leveraging McAfee's NitroSecurity (or Enterprise Security Manager) toolset for administration, operations, and advanced correlation.
l. Support the Host Assessment Team (HAT) to analyze systems on the MCEN to identify vulnerabilities, anomalous host behavior, compromised network hardware and advanced malware.
m. Provide support required to maintain the MCCOG's CNDSP accreditation per the standards set forth in the CNDSP program manual, DoD O-8530.1-M, (dated 17 Dec 03 or later) to include documentation and technical writing support as needed.

C.4.3.3 SUBTASK 3 – SIGNATURE MANAGEMENT AND DEVELOPMENT

The Contractor shall be responsible for the continuous development and refinement of signatures, policies, configurations, scripts and indicators used to identify malicious or unauthorized activity via network, host, and scanning based detection on the MCEN. The Contractor shall directly maintain and evolve the MCEN's network defense detection strategy to keep pace with emerging threats and adversarial techniques, for both internal and external networks, as well as host based security.

The Contractor shall:

a. Create and maintain and refine the body of documentation that describes DCOS Signature Maintenance and Development tactics, techniques and procedures (Section F, Deliverable 16).
b. Provide subject matter expertise in creation, editing, and management of signatures, rules and filters for specialized network defense systems including but not limited to network and host-based IDS, IPS, firewall, web application firewall, proxy and SIEM systems.
c. Coordinate with the DCOS Incident Management Section to manage required changes to the signatures, rules and filters of specialized network defense systems.
d. Identify potential conflicts with implementation and integration of specialized network defense systems within the network to protect the overall availability of the MCEN.
e. Using a government provided facility and government provided hardware, the Contractor shall administer and develop a test environment to evaluate new applications, signatures, rules, filters and configurations of managed network defenses systems.
f. Perform life-cycle configuration management of applications, signatures, rules, filters and configurations of managed network defenses systems.
g. Support enterprise mitigation efforts based on the specific monitoring and filtering capabilities of existing network defense infrastructure.
h. Conduct in-depth traffic analysis of documented covert channels to create tailored response signatures.
i. Provide a visual baseline display of CND events of interest from all applicable data sources, to enable the detection of significant events for the Watch Analysts.

j. Improve SIEM correlation rules employing events from multiple data sources to provide more reliable CND alerts.
k. Maintain a test environment with all DCOS signature-based applications and innovate techniques to detect events of interest in the MCEN.
l. Manage and improve the Marine Corps' defensive detection strategy through the deployment of new signature policies and robust correlation rules for the SIEM (prioritize the network event view for the Watch Analyst team).
m. Provide Database Administrators and Developers to support Marine Corps network defense databases and supporting systems, including administer, maintain (backups, stigs, patches, etc), and develop and implement custom capabilities in structured query language (SQL), .NET and VB .NET
n. Support the Host Assessment Team (HAT) in a weekly analysis of systems on the MCEN to identify vulnerabilities, anomalous host behavior, compromised network hardware and advanced malware.
o. Provide support required to maintain the MCCOG's CNDSP accreditation per the standards set forth in the CNDSP program manual, DoD O-8530.1-M, (dated 17 Dec 03 or later) to include documentation and technical writing support as needed.

C.4.3.4 SUBTASK 4 – INFORMATION ASSURANCE (HOST ASSESSMENT)

The Contractor shall perform all functions in executing vulnerability management, to include the operation of the MCEN's Information Assurance Vulnerability Management (IAVM) program for DCOS-maintained systems. The Contractor shall be responsible for DCOS' operation of the IAVM program and shall align with the CJCSM 6510.01B, "Cyber Incident Handling Program," dated 10 July 2012 or later.

The Contractor shall:

a. Perform weekly vulnerability audits (Section F, Deliverable 20), submit Plans of Action and Milestone (POA&M) and assist with patching for all DCOS systems in order to maintain compliance with operational directives.
b. Conduct malicious file scanning and report findings monthly for identification of potentially compromised systems (Section F, Deliverable 18).
c. Maintain the certification and accreditation documentation (DoD IA Certification and Accreditation Process / Risk Management Framework) for all specialized network defense systems and software used on the MCEN in accordance with applicable DoD policies.
d. Support the Host Based team to identify anomalous network and host activity across the MCEN.

C.4.4 TASK 4 – DCOS SUPPORT OPERATIONS

The Contractor shall be responsible for support and sustainment functions to DCOS operations to include, Knowledge Management and Portal Administration, Mitigation Action, and Training.

C.4.4.1 SUBTASK 1 – KNOWLEDGE MANAGEMENT AND PORTAL ADMINISTRATION

The Contractor shall be responsible for knowledge management activities in support of DCOS operations. The Contractor shall develop and refine DCOS standard operating procedures, design and improve information sharing throughout DCOS, and coordinate training/exercise planning for all DCOS personnel (Military, Civilian, and Contractor). The Contractor shall be responsible for continuity of services as data sources evolve to changes in the Marine Corps' technical computing environment as well as by mandates from USCYBERCOM.

The Contractor shall:

a. Maintain the body of documentation that describes the tactics, techniques and procedures that comprise the DCOS Knowledge Management team (Section F, Deliverable 16).
b. Create, edit, and manage a DCOS collaborative SharePoint site to coordinate operations, documentation, and training.
c. Coordinate schedule and logistics for all DCOS training, exercise, and travel in support of operational requirements.
d. Coordinate and manage internal training calendars via NIPRNET EKO, post and advertise available classes (See attachment T for a Sample Training Calendar).
e. Advise and assist all personnel with their applicable position training requirements and assist all personnel in registration of training classes via DCOS training calendar and/or through a third-party vendor.
f. Administer all aspects of the DCOS web presence, to include development and refinement of the current Sharepoint instances and any future requirements.
g. Maintain format and content for the existing DCOS Training and Exercise Employment Plan (TEEP); Collect internal updates and publish weekly for internal information awareness.
h. Maintain the DCOS personnel recall roster and POC databases.
i. Track the DCOS personnel training; collect internal updates and publish weekly for internal awareness.
j. Format correspondence, briefs, and operational products per the standards set forth in the Secretary of the Navy Manual (SECNAV-M) 5216.5, “Department of the Navy Correspondence Manual,” dated March 2010 or other organizational standard.
k. Develop and manage the methods to capture, share, and better utilize DCOS organizational knowledge.

C.4.4.2 SUBTASK 2 – MITIGATION ACTION

The Contractor shall be responsible for providing a capability to develop and execute enterprise remediation measures that reduce the impact of vulnerabilities and mitigate risk to the enterprise network. Historically, MCCOG processes approximately 2000 intelligence reports and 360 waivers for access to Internet web sites per year. Approximately 1 briefing and 2 reports documenting mitigation actions are developed per week.

The Contractor shall:

a. Create and maintain the body of documentation that describes the tactics, techniques and procedures that comprise the Mitigation Action Team (Section F, Deliverable 16).
b. Coordinate and track requirements levied upon the DCOS from external commands / agencies and internal MCCOG sections to ensure actions are completed as required.
c. Develop and implement enterprise mitigation actions in response to intelligence reports, complex vulnerabilities, threats and risks.
d. Manage, prioritize and resolve all open enterprise mis-configurations, by tasking and supervising actions necessary per DoD policy and IA / CND best practices.
e. Perform trend analysis of all available reporting within the DCOS to include review of open/closed incidents, identified exploits, and scan results.
f. Provide reports and briefings documenting mitigation actions in appropriate organizational templates.
g. Maintain a historical record detailing existing network boundary policy configurations and network perimeter security compliance.

h. Review and recommend updates to network/system configurations in response to changes in the threat environment (identified trends, IA vulnerability alerts / bulletins / technical advisories, known malicious files, zero day exploits, etc.), as appropriate.
i. Develop and maintain usable strategies that leverage existing infrastructure to provide improved defenses to the MCEN.
j. Document and maintain the cross-organizational tactics, techniques, and procedures required to implement these strategies.
k. Develop and implement strategies to compress the software vulnerability life-cycle.
l. Identify, monitor, and audit relevant enterprise cyber key terrain to protect the MCEN.
m. Conduct defensive cyber operations planning utilizing the Marine Corps Planning Process, per the standards set forth in the Marine Corps Planning Process, MCWP 5-1 (dated 24 August 2010) to include documentation and planning support as needed.
n. Provide support required to maintain the MCCOG's CNDSP accreditation per the standards set forth in the CNDSP program manual, DoD O-8530.1-M, (dated 17 Dec 03 or later) to include documentation and technical writing support as needed.

C.4.4.3 SUBTASK 3 – RED TEAM (MCIART)

The Contractor shall be responsible for providing operational network exploitation and cyber threat emulation testing support towards local area network and wide area network systems and components and shall align with the NIST 800-115 (dtd 30 Sep 2008 or later) and the CJCSM 6510.03 (dtd 28 Feb 2013). The MCIART conducts approximately 10-15 full scale Red Team operations per year and 15 remotely executed and short duration small scale "sprint" operations. This support consists of the development of custom malware in support of targeted operations that range from two weeks in duration to operations that last approximately four to six weeks in duration. These operations evaluate and assess the security posture of individual units both in garrison and deployed (small scale operations) as well as assessments of the Marine Corps Enterprise Network (large scale operations). Additionally, the MCIART participates in approximately 8 DOD cyber exercises per year.

The Contractor shall:

a. Create and maintain the body of documentation that describes MCCOG Red Team's formal network penetration methodology (Section F, Deliverable 16).
b. Review and refine methodologies to successfully conduct Red Team operations.
c. Develop plans to successfully conduct network exploitation, penetration testing, cyber threat emulation and Red Team operations.
d. Conduct no-notice and cooperative Red Team assessments and operations.
e. Develop and submit detailed reports of findings, analysis and recommendations.
f. Research existing exploit code and/or develop proof-of-concept or exploit code for test and evaluation of mitigations solutions.
g. Develop and maintain custom applications (malware development) to support mission requirements to ensure Command and Control during Red Team operations.
h. Identify potential network and system vulnerabilities and mis-configurations through the use and expert employment of all available MCEN scanning and discovery systems (Section F, Deliverable 32).
i. Provide the support required to maintain the MCCOG's NSA certification/USCYBERCOM accreditation per the standards set forth in the CJCSM 6510.03 (dtd 28 Feb 2013), to include documentation and technical writing support as needed.

C.4.5 TASK 5 – TRAINING (OPTIONAL TASK)

The MCCOG has implemented a workforce training program aligned to the DOD Directive 8570.01-M "Information Assurance Workforce Improvement Program" (dated 24 Jan 2012 or later). The workforce training program supports adherence to the manual for obtaining appropriate certifications, training and ongoing skills development required of the information assurance workforce. The Contractor is a partner in accomplishing the program's objectives and is responsible for maintaining a qualified workforce and supporting delivery of the MCCOG training program. The Contractor is expected to identify, develop, and implement additive defensive cyber training that advances the workforce's efficacy beyond initial training requirements. The Contractor shall assist the MCCOG in constantly updating the training standard in order to keep pace with the maturation of defensive cyber operations. In addition, the Contractor may be required to attend cyber-related training events/conferences in support of the cyber defense program.

The Contractor shall:

a. Develop and implement a training plan (referred to as Training Management Plan in Section F, Deliverable 09) that complies with the requirements of each position as outlined by the training requirements in Table 1 below (also refer to DoD Directive 8570.01-M "Information Assurance Workforce Improvement Program" (dated 24 Jan 2012, or succeeding DoD training directive)). The Training Management Plan shall describe how the Contractor will achieve the DCOS training described in Table 1 (DCOS Internal Training, DoD 8570 Information Assurance track and DoD 8570 CNDSP track) for each contractor employee. The offeror's plan shall ensure that the three applicable training tracks are met within 180 days of employee hire. The Training Management Plan shall list all current certifications held by key and non-key personnel and articulate how it will maintain a certified workforce through the duration of the TO.

b. Deliver DCOS Internal Training (Table 1, Column B):
    - Provide courseware maintenance and course materials in support of Watch Team, Incident Response, Advanced Incident Handling, Hunt, Malware and Forensics, Exploit Analysis, Host Based Security, Network Sensor Support, Signature Development, Mitigation Action, and Red Team (Section F, Deliverable 22).
    - Provide instructor to deliver courseware from associated task and subtask areas (Watch Team, Incident Response, Advanced Incident Handling, Hunt, Malware and Forensics, Exploit Analysis, Host Based Security, Network Sensor Support, Signature Development, Mitigation Action, and Red Team) for all DCOS training. Instructors must be actively supporting the task area for which they instruct training. Each course is to be taught approximately once a quarter (See attachment T for a Sample Training Calendar).

c. Develop and maintain a Defensive Cyber Operations Training and Readiness (T&R) manual per the standards set forth in Marine Corps Order P3500.72A, "Marine Corps Ground Training and Readiness (T&R) Program," dated 18 April 2005 or later (Section F, Deliverable 33). The objective of a DCOS T&R manual is the generation of operational standards for defensive personnel and the training regimens which accomplish those standards. A final product should provide individual, team, and section standards. As DOD and DCOS training requirements change, the T&R shall be updated accordingly.

d. Develop and implement scenario based training (SBT) for each task requiring training. SBT's, also referred to as Tactical Decision Games (TDG), are collaborative group events intended to evaluate the performance of groups in response to a select problem drawn from common operational events (Section F, Deliverable 34). The scenarios evaluated should be nested in the Defensive Cyber Operations Training and Readiness (T&R) manual that the Contractor develops. At a minimum, the scenarios should evaluate the team's proficiency of execution for each MCCOG Tailored Readiness Option, Internal Defensive Measure, and Defensive Counter-Measure. The Contractor shall deliver this training to all personnel in each DCOS section on a quarterly basis.

e. Personnel Training Certification Requirements: (Table 1)

DISCOVERY AND COUNTER-INFILTRATION	DCOS INTERNAL TRAINING	DoD 8570 IA TRACK	DoD 8570 CNDSP TRACK
D&CI Technical Lead	WA, HCI and IR Courses	IAT LVL 3	CND Analyst
Cyber Watch/Incident Response	WA, HCI and IR Courses	IAT LVL 2	CND Incident Responder
Advanced Incident Handling	IS, HCI and IR Courses	IAT LVL 3	CND Auditor
Malware And Forensics	WA, HCI and IR Courses	IAT LVL 3	CND Incident Responder
Exploit Analyst	WA, IR, HCI, and ALL SGS Courses	IAT LVL 3	CND Auditor
Hunt Tech	WA, IR, Red Team Level I & II	IAT LVL 3	CND Auditor
SENSOR GRID	**DCOS INTERNAL TRAINING**	**DoD 8570 IA TRACK**	**DoD 8570 CNDSP TRACK**
Sgs Technical Lead	WA, HCI all IS	IAT LVL 3	CND Infrastructure Support
Network Sensor Support	WA, HCI and SGS Courses	IAT LVL 2	CND Infrastructure Support
Signature Management	WA, HCI, IR and all IS Courses	IAT LVL 3	CND Analyst
Database Administrator	WA, HCI and all IS Courses	IAT LVL 2	CND Infrastructure Support
Developer	WA, HCI and all IS Courses	IAT LVL 2	CND Infrastructure Support
Host-Based Sensor Tech	WA, HCI, IR, and all SGS Courses	IAT LVL 2	CND Infrastructure Support
DCOS SUPPORT OPERATIONS	**DCOS INTERNAL TRAINING**	**DoD 8570 IA TRACK**	**DoD 8570 CNDSP TRACK**
Mitigation Action Team	WA, HCI and IS Courses	IAT LVL 2	CND AUDITOR
Knowledge Management	WA and HCI Courses	Not Required	Not Required
Portal Admin	WA and HCI Courses	Not Required	Not Required
Red Team Developer	WA, HCI and IS Courses	IAT LVL 2	CND IASAE

Key (Personnel Training Courses)	
WA: Watch Analyst	IS: Sensor Grid Support (MIST/SGS)
IR: Incident Response	IAM: Information Assurance Management
HCI: Handling Classified Information	IAT: Information Assurance Technical

C.4.6 TASK 6 – SURGE SUPPORT (OPTIONAL TASK)

The contractor shall provide a surge capability and support for MCCOG Cyber Defense requirements and systems. The contractor shall be prepared to provide staff resource support for unanticipated, as-needed surge support requirements for the following sections: cyber watch, incident response, advanced incident handling, mitigation action, information assurance, signature management and development, network sensor support, host sensor technicians, cyber threat analysis cell, hunt team, red team, database administrators, tool development and deployment, and training on short notice (i.e. few days to a month based on urgency). The general expectation is for the contractor to respond within 10 to 14 days of the surge request.

The contractor shall provide a Surge Support Plan (Section F, Deliverable 24) which identifies its procedures and timelines for providing surge support to the Government. Surge support shall be defined by milestones and last no longer than six months in duration without the approval of the CO. The process for initiating surge support shall be completed on a case-by-case basis, approved by the Government.